OVERVIEW
Email has become the primary media to drive core business communications and in today’s complex business world of acquisitions, mergers, compliance regulations and the never ending onslaught of malicious software, information technology (IT) organizations are struggling to keep up with the demands on messaging infrastructures. The requirements for email infrastructure, sophisticated message routing, content protection, security, and network performance have changed dramatically. In addition to traditional inbound spam and virus protection, internal policy and routing decisions and outbound risks associated with confidential information leaks have become critical issues for organizations.

Given today’s economic realities, IT Administrators are looking for ways to address all of these challenges while achieving a compelling Return-on-Investment on their messaging infrastructure investments. They seek solutions that address the requirements of the Internal Policy and Message Routing infrastructure as well as the External Protection/Email Gateway. The solution must be flexible, easy-to-manage and provide scalable and reliable email delivery, virus and spam protection, advanced content filtering and fully-integrated encryption.

SENTRION MESSAGE PROCESSORS
Sentrion Message Processors are high-performance message security appliances that provide a unified solution to the complex problems of policy-based message handling and routing. Sentrion is available in a hard appliance (Sentrion MP & DS), virtual appliance (Sentrion MPV) and blade server (Sentrion MPQ) configurations. Global 2000 organizations are using Sentrion Message Processors to modernize their

Sentrion Message Processors
• External Protection/Gateway Management
• Inbound Message Processing
• Internal Policy and Routing
• Outbound Data Leak Prevention
• Email Authentication
• Intra-company Groupware Routing and Policy Enforcement
messaging infrastructure and to reduce the cost and complexity of securing and managing their corporate email.

**Sentron is a Purpose-built, High-Performance Message Processing Appliance for:**

- **External Protection:** Bi-directional message encryption and sophisticated connection controls prior to inbound processing
- **Inbound Message Processing:** Spam, virus and malicious software protection
- **Internal Policy and Routing:** Intelligent policy-driven message handling and routing
- **Outbound Data Leak Prevention:** Highly accurate, in-line content monitoring and enforcement to prevent data loss and compliance breaches
- **Email Authentication:** Authenticates all incoming and digitally signs all outgoing messages with Domain Keys Identified Mail (DKIM), and other authentication mechanisms to certify email senders
- **Message Management for Multiple and Mixed Groupware Environments:** Enforces intra-company/division content policies and provides policy-based message routing for MS Exchange, IBM Lotus Domino, etc.

Policy applications can be added to Sentron to monitor and enforce outbound messages for:

- Corporate governance
- Regulatory compliance
- Privacy violations
- Data leak prevention

**FEATURES AND FUNCTIONALITY**

The Sentron Appliance Key Functions Include:

**Enterprise-class high-performance architecture**

- 64-bit hardware and operating system
- Available as a hard appliance (MP), virtual appliance (MPV), and Blade Server (MPQ)
- 8/16GB Memory
- RAID Storage
- Enterprise clustering and scalability
- LDAP directory services and integration

**High-performance industry-standard sendmail Mail Transfer Agent (MTA) and intelligent Gateway Connection Controls**

- High throughput, intelligent message routing
- Sophisticated gateway message controls to secure, monitor and regulate message traffic and block unwanted messages
- Fully-integrated email authentication including the only IETF approved standard – Domain Keys Identified Email

**Centralized policy management with highly accurate and intelligent policy engine**

- Flexible clustering support for global enterprise, corporate and departmental policy management and enforcement
- In-line, deep content inspection
- Extract and analyze 300+ file types including Microsoft Office 2007 files
- Intelligent rules policy engine to fulfill virtually any business policy requirement
- Policy versioning and change control for easy roll-back

**Centralized Reporting**

- Single centralized reporting data aggregation function with template-based report tools
- Configurable data retention period based on data aggregation intervals
- On-demand report execution allowing users to filter a given report by date/time, host and message direction
- Export reports in multiple formats including PDF, HTML and CSV
- Schedule reports for email delivery on a daily, weekly or monthly basis. Includes several reports with configurable output formats

**System Monitoring**

- System and application level monitoring including hardware, OS and all Sentron components. Monitors and reports on vital stats (CPU, disk space, queued messages)
- Optionally integrate with SNMP enterprise system monitoring solutions. Supports a MIB for external monitoring devices

August 2009
Configuration Version Control
• Track and manage all system configuration changes with support for full roll-back and configuration tagging
• Make incremental configuration changes; commit and deploy to all hosts with a single operation

Role-based Access Control and User Interface
• Gives individual business stakeholders custom reporting views
• Provides collaboration workflow between functional groups

Integrated End-User Spam Quarantine
• Integrated Spam Quarantine for end-user disposition of spam as well as other suspect email

Multi-Protocol Support
• Monitor and report on multiple protocols and applications such as HTTP, FTP, HTTP Webmail, and more. Supports a standard interface for integration with most proxies over ICAP to provide real-time feedback

Document Fingerprinting
• Register sensitive files to Sentrion for whole/partial match scanning of all messages leaving the network. Enables detection and protection of confidential data such as legal disclosures, financial data, strategic planning, or any other sensitive information

SAN Support
• External storage integration to increase the overall capacity and retention for data stored within the system. This applies both to logs, and data as well as quarantined messages for administrators and end-users

Centralized Cluster Deployment
• Centralize cluster management framework for all MPE components in a single interface
• Manage a single cluster from one designated master

Easy to Use Graphical User Interface
• Intuitive UI for system administrators and business users

Sentrion Reporting Dashboard

Sentrion Device Monitoring Dashboard

Sentrion Policy Management Dashboard

August 2009
OPTIONAL APPLICATIONS

Fully-integrated functional applications can be added to Sentrion’s core system to provide additional gateway protection and organization specific messaging requirements.

Regulatory Compliance Policies

- Highly accurate out-of-the-box polices for compliance, acceptable use and confidential information protection
- Bundled policies include:
  — Sarbanes-Oxley, Gramm-Leach-Bliley, CA SB1386, HIPAA, ITAR, Explicit Language, PCI, and more

Incidence Remediation and Reporting

- Enables both technical and business-level views into policy-based events for both reporting and remediation
- Enterprise clustering support provides integrated and centralized reporting for incident trends and compliance
- Detailed drill-down reports for greater incident and attack analysis

Multiple best-of-breed Anti-spam Applications

- Remediation workflow for incident response best practices
- Quarantine provides a unified view for both administrators and end-users to inspect and remediate spam and other message deemed to be held for user analysis

Multiple best-of-breed Anti-virus Applications

- Anti-virus protection
- Zero-hour virus detection

FIGURE 1. Sentrion MP provides both external protection and internal policy management and routing.
Reputation Services

- IP and Domain-based reputation services detection by leveraging metrics on the sender domain's email behavior, collected from several sources
- Integrated domain-based reputation intelligence from Habeas to identify sender domains as trusted, legal entities with Domain Keys Identified Mail (DKIM) signatures
- Increases security by filtering the majority of email-borne viruses, worms and trojans at the Gateway before entering the network
- Saves bandwidth and enhances performance and guarantees better Quality of Service for the remaining traffic

Policy-driven Message Encryption

- Enables administrators to provide secure messaging of confidential or otherwise critical information to satisfy business and compliance requirements without affecting user behavior — using TLS, S/MIME and embedded Voltage IBE technology for multiple encryption options
- In-line, single appliance message encryption with no client software
- Reduces overall administration, infrastructure and integration requirements by consolidating all encryption functions into a single appliance
- Minimizes end-user dependency by enforcing enterprise encryption policy at the gateway and/or internal policy layer through Sentrion’s intelligent policy engine

**BENEFITS**

<table>
<thead>
<tr>
<th>Purpose-built, high-performance architecture gives proven high ROI</th>
<th>Enables administrators to provide secure messaging of confidential or otherwise critical information to satisfy business and compliance requirements without affecting user behavior — using TLS, S/MIME and embedded Voltage IBE technology for multiple encryption options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides accuracy and protection where 80 percent of security and compliance violations occur – in inbound and outbound email communications</td>
<td>In-line, single appliance message encryption with no client software</td>
</tr>
<tr>
<td>Compliance policies enable immediate policy enforcement based on industry best practices</td>
<td>Reduces overall administration, infrastructure and integration requirements by consolidating all encryption functions into a single appliance</td>
</tr>
<tr>
<td>Centralized policy management for global enterprise policy enforcement and incident remediation without interrupting business process workflow</td>
<td>Minimizes end-user dependency by enforcing enterprise encryption policy at the gateway and/or internal policy layer through Sentrion’s intelligent policy engine</td>
</tr>
<tr>
<td>Intuitive user interface that does not require any training or extensive prior knowledge of the Sentrion components</td>
<td></td>
</tr>
<tr>
<td>Quickly and accurately make key messaging related decisions and conclusions based on extensive reporting and data availability</td>
<td></td>
</tr>
<tr>
<td>Satisfy both administrators and management with detailed, yet intuitive reporting templates</td>
<td></td>
</tr>
<tr>
<td>Platform for future growth and easy integration with existing messaging infrastructure</td>
<td></td>
</tr>
<tr>
<td>Optional add-on applications provide flexibility for changing requirements</td>
<td></td>
</tr>
<tr>
<td>Enterprise-scale with proven performance and reliability</td>
<td></td>
</tr>
<tr>
<td>Easy-to-manage unified architecture for centralized management</td>
<td></td>
</tr>
<tr>
<td>Reduce on-going administration of the hardware, OS and applications by monitoring all hosts through a centralized interface and proactive alert notifications</td>
<td></td>
</tr>
<tr>
<td>Advanced policy management to map any compliance or enterprise security policy</td>
<td></td>
</tr>
</tbody>
</table>

August 2009
FIGURE 2. Sentrion MP Specifications

<table>
<thead>
<tr>
<th>Component</th>
<th>Sentrion MP 351</th>
<th>Sentrion MP 352</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>1U</td>
<td>2U</td>
</tr>
<tr>
<td>Hardware Architecture</td>
<td>32/64 bit</td>
<td>32/64 bit</td>
</tr>
<tr>
<td>Software Architecture</td>
<td>64 bit</td>
<td>64 bit</td>
</tr>
<tr>
<td>CPU</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1x Quad Core Intel Xeon X5550, 8MB Cache, 6.4 GT/s, 2.66 GHz, TurboHT</td>
<td>2x Quad Core Intel Xeon X5550, 8MB Cache, 6.4 GT/s, 2.66 GHz, TurboHT</td>
</tr>
<tr>
<td>DVD Drive</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RAM</td>
<td>8GB 1066MHz (2X4GB), Dual Ranked UDIMMs</td>
<td>16GB 1066MHz (2X8GB), Dual Ranked UDIMMs</td>
</tr>
<tr>
<td>Operating System Disks</td>
<td>2 x 146 GB @ 15K rpm SAS -2.5” Hot Plug</td>
<td>2 x 146 GB @ 15K rpm SAS – 3.5” Hot Plug</td>
</tr>
<tr>
<td>Data Disks</td>
<td>Share with Operating System</td>
<td>4 x 146 GB @ 15K rpm SAS – 3.5” Hot Plug</td>
</tr>
<tr>
<td>RAID</td>
<td>RAID 1 (# 0 and 1)</td>
<td>RAID 1 and 5 (# 2,3,4,5)</td>
</tr>
<tr>
<td>On-board NIC</td>
<td>Broadcom 4 port GB Ethernet</td>
<td>Broadcom 4 port GB Ethernet</td>
</tr>
<tr>
<td>Add-on NIC</td>
<td>Intel PRO 1000PT 1GB Duel Port, PCIe-4</td>
<td>Intel PRO 1000PT 1GB Duel Port, PCIe-4</td>
</tr>
<tr>
<td>Remote Management</td>
<td>iDRAC6 Enterprise</td>
<td>iDRAC6 Enterprise</td>
</tr>
<tr>
<td>Power Supply</td>
<td>High Output Redundant 717W</td>
<td>High Output Redundant 717W</td>
</tr>
<tr>
<td>Internal USB</td>
<td>4GB</td>
<td>4GB</td>
</tr>
</tbody>
</table>

Also available as a virtual appliance with Sentrion MPV, a blade server with Sentrion MPQ and as a SaaS offering with Sentrion Cloud Services. See the Sentrion MPV, MPQ, DS and Cloud Services fact sheets for additional specifications.
SUMMARY
Sentrion’s high-performance in-line Message Processor delivers enhanced messaging security without impacting network performance. It provides large enterprises with protection from inbound threats at the messaging gateway, while monitoring and enforcing outbound messages for corporate governance, regulatory compliance, privacy violations, and data leak prevention. Sentrion MP provides bi-directional message inspection and protection where over 80 percent of data loss, compliance violations, and threats occur — within corporate email messaging environments.

About Sendmail
Sendmail provides appliance-based products, applications and services that enable enterprises and government agencies to modernize their messaging infrastructures. Since 1982, thousands of commercial and open source customers around the globe have relied on Sendmail for a unified approach to the complex problems of policy-based message handling and routing. The company’s comprehensive suite of applications addresses the challenges of gateway management, inbound threat protection, data leak prevention, email authentication and intra-company message management. These applications run on Sendmail’s family of Sentrion® Message Processors, which are available in hard appliance, virtual appliance and blade server configurations. Sendmail is headquartered in Emeryville, CA with sales and support offices throughout the Americas, Europe, and Asia.

CONTACT US
For more information or to setup a demonstration, contact us at sales@sendmail.com, or phone 877-363-6245. Also ask us about our Risk Assessment Program.